Message Encryption

By:

Shashi Ranjan (278)

Anand Kumar (213)

Group No- 23

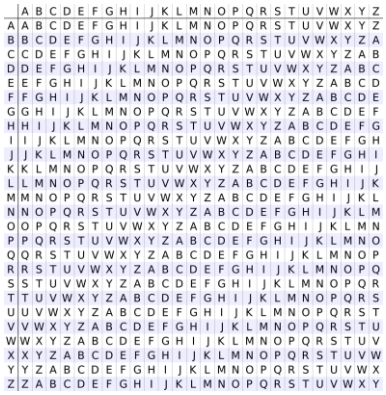
Problem Statement:

Develop a GUI based application to encrypt and decrypt a message. Implement any encryption & decryption algorithm and display different phases of your result in the front-end.

Approach:

Vigenère cipher:

To encrypt, a table of alphabets can be used, termed as *Vigenère square* or *Vigenère table*. It has the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

The letter at the intersection of [key-row, msg-col] is the enciphered letter.

Our Modification:

Instead of just 26 capital letters, A-Z, small letters(a-z), numbers (0-9) and special characters have been added to improve the method's capability of encryption & decryption.

Functionality:

Upon running the app, user gets two options viz. “Encryption” & “Decryption”.

After clicking upon either of the two provided options, user is directed to a new window containing methods for message insertion. Depending on the method selected, user need to either type in the text in the provided field or select one from the device.

User also require to provide a password for the encryption/decryption of the given text which is required later at the time of decryption/encryption.

Encrypted/decrypted texts can be saved to the device by clicking upon the “Save” button, appears after clicking the “Encrypt” / ”Decrypt” button.

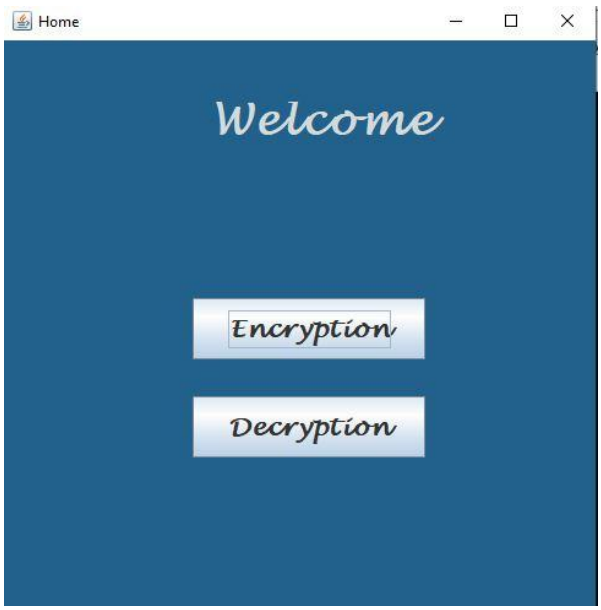
All ongoing actions/steps can be seen in the console on right-side of the screen.

Java In-built packages used:

- Java Swing
- Java AWT
- Java IO

Output Screens:

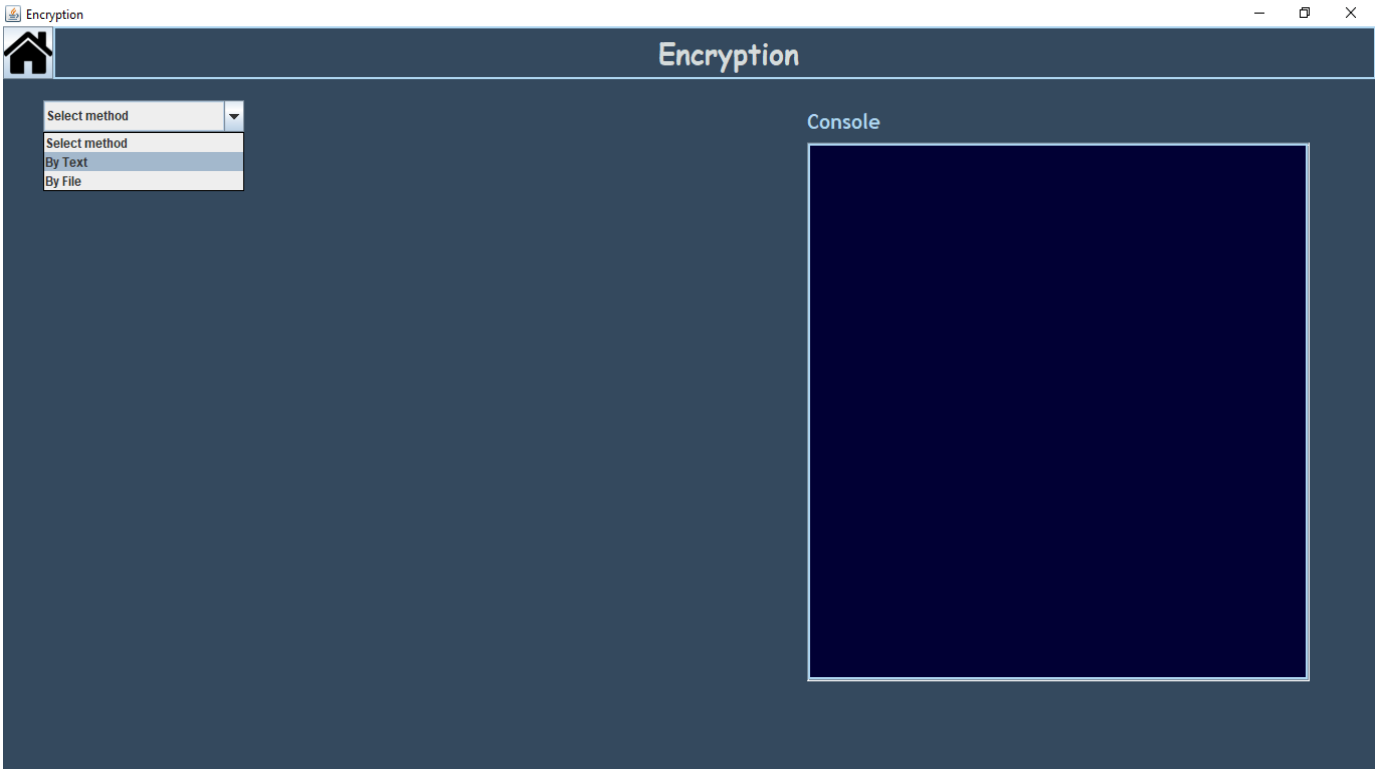
Home Screen:



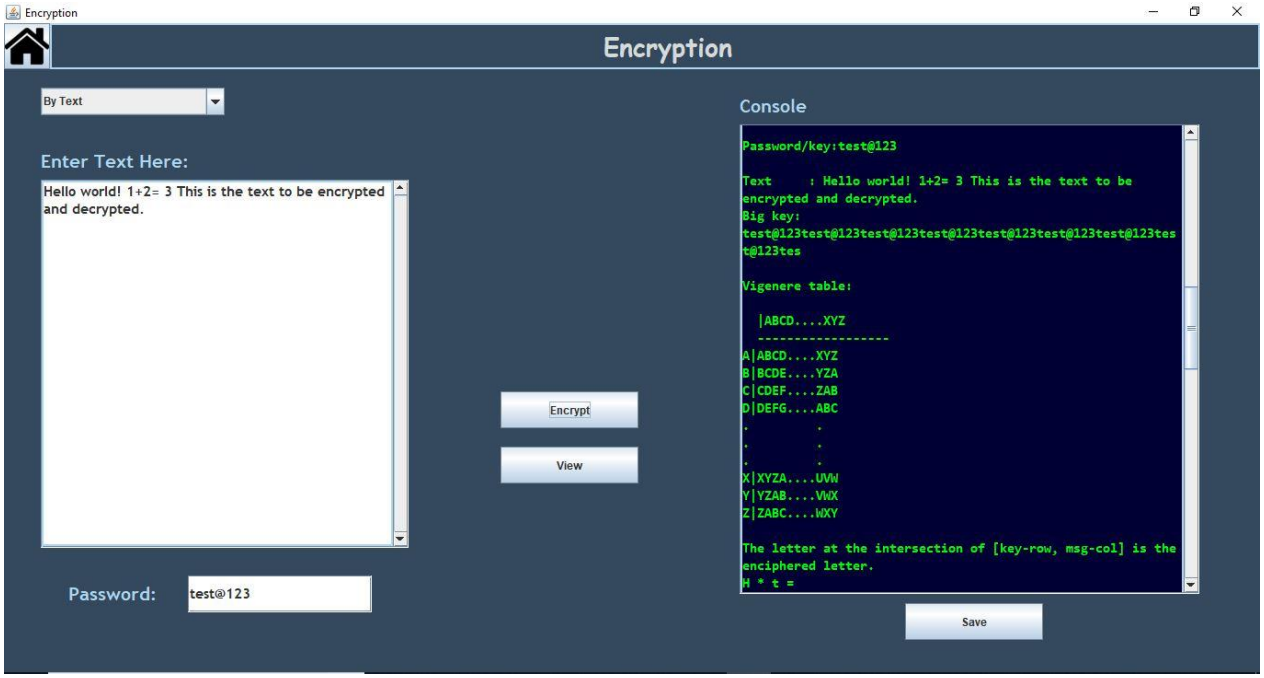
Encryption Screen:

Select method:

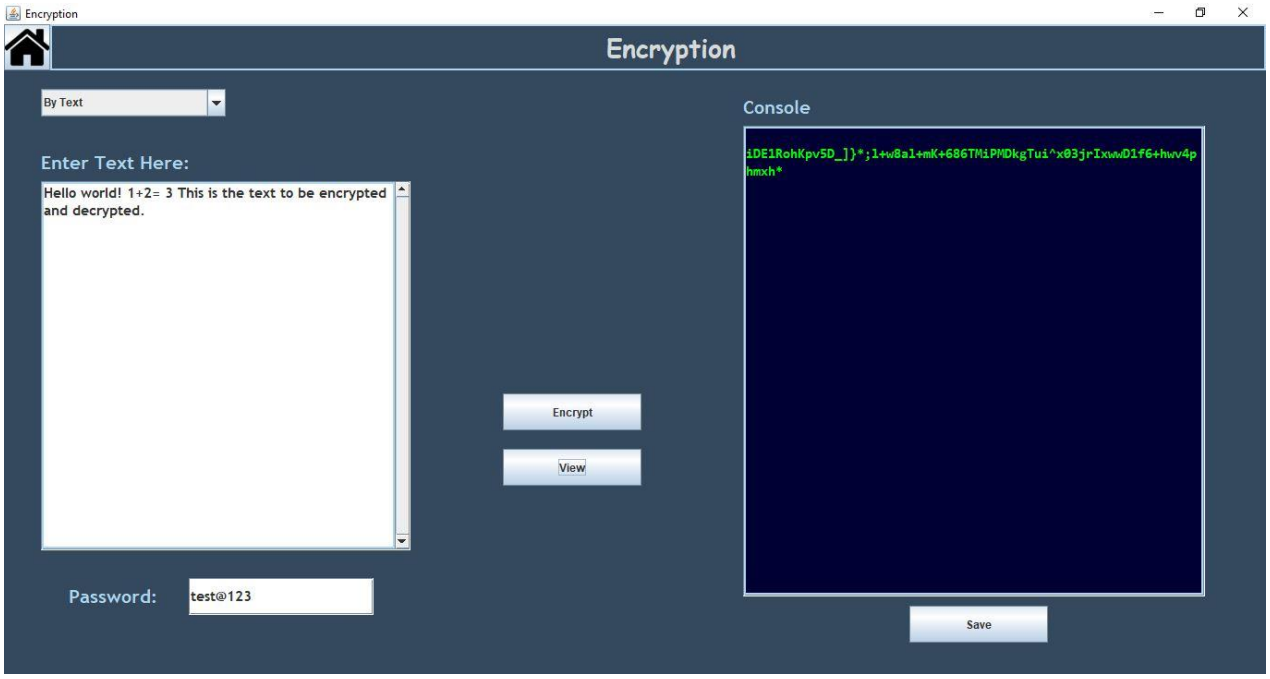
- **By Text**
- **By File**



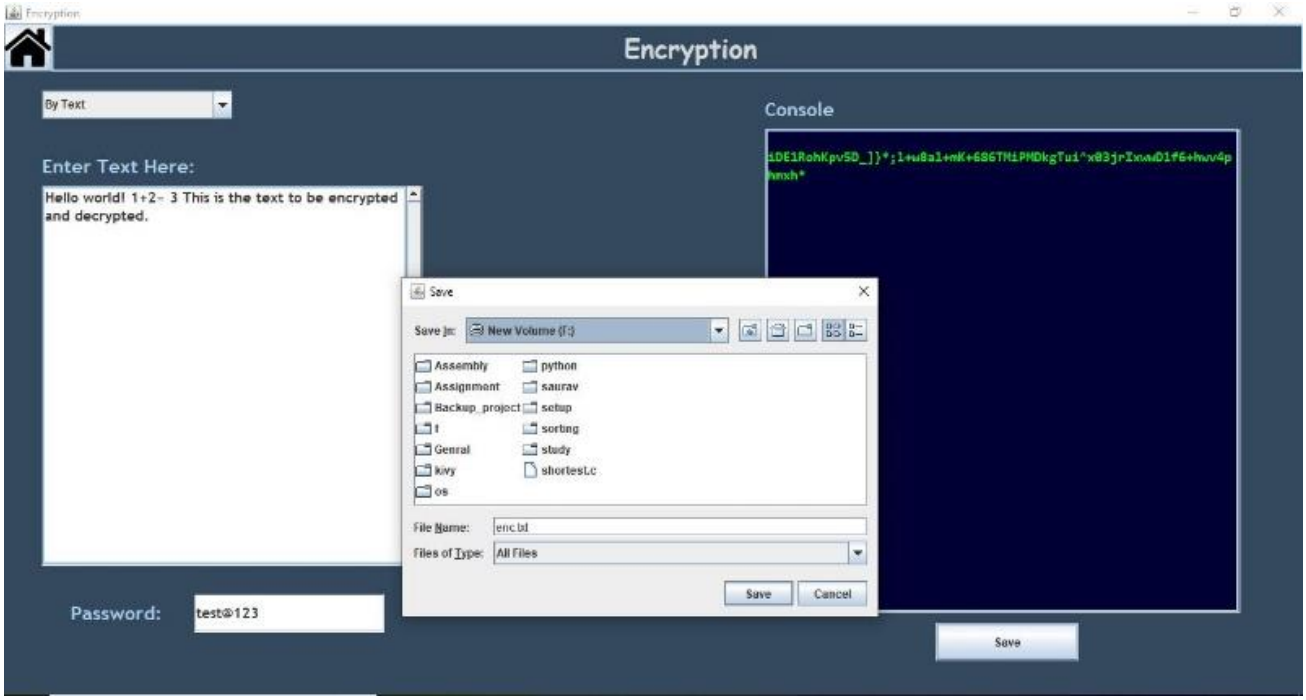
Here user can select one of the two method. On selecting "By text" user can enter in text area and provide a password and then click the encrypt button. All steps will be printed in console as shown in following picture:



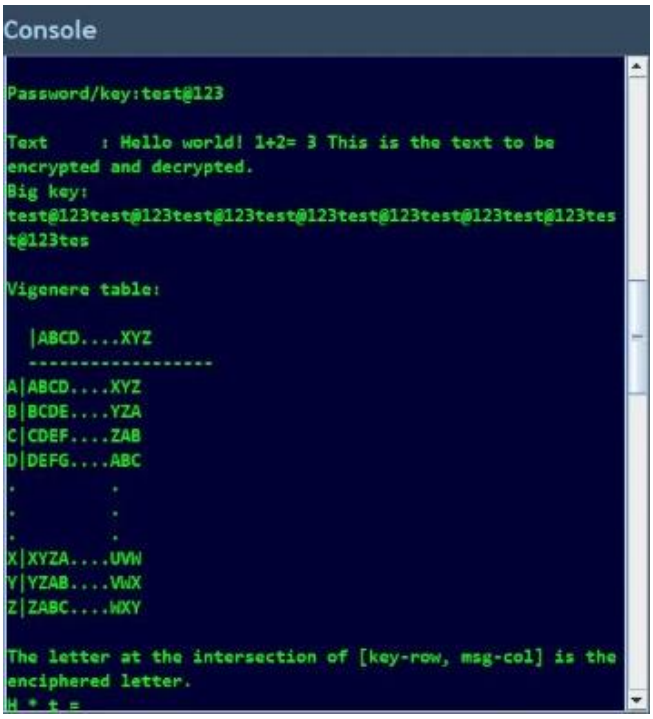
On pressing “View” users can see the encrypted text in the console:

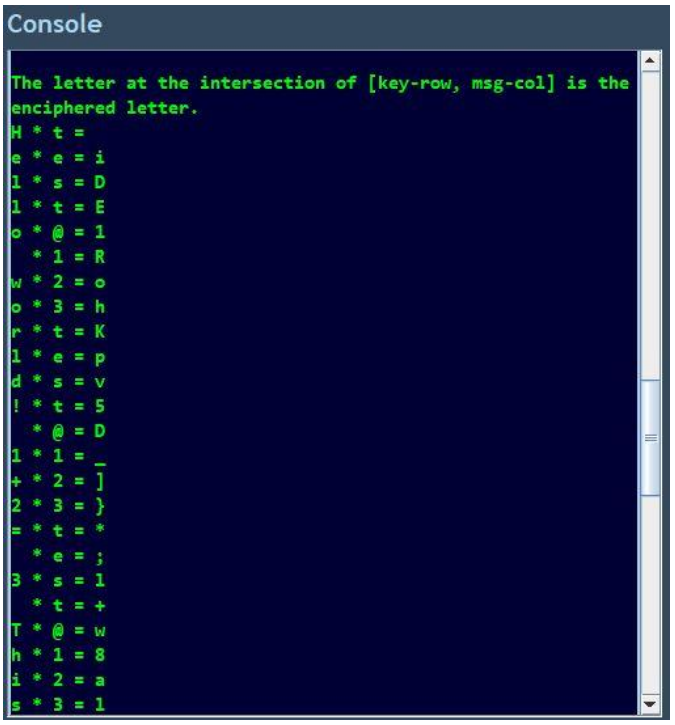


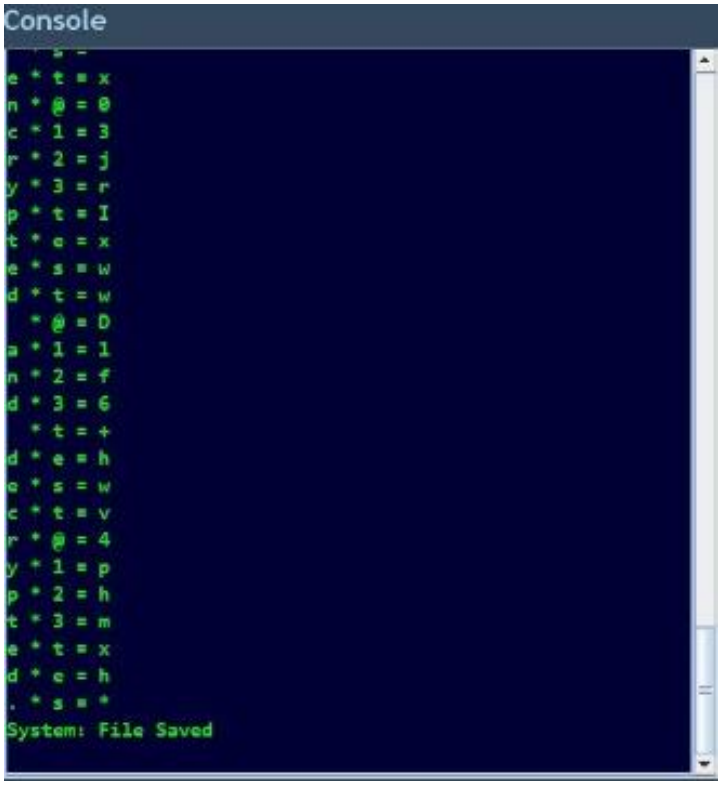
Users can save the encrypted text in a file by pressing “Save” button:



These are the steps of encryption printed in console.

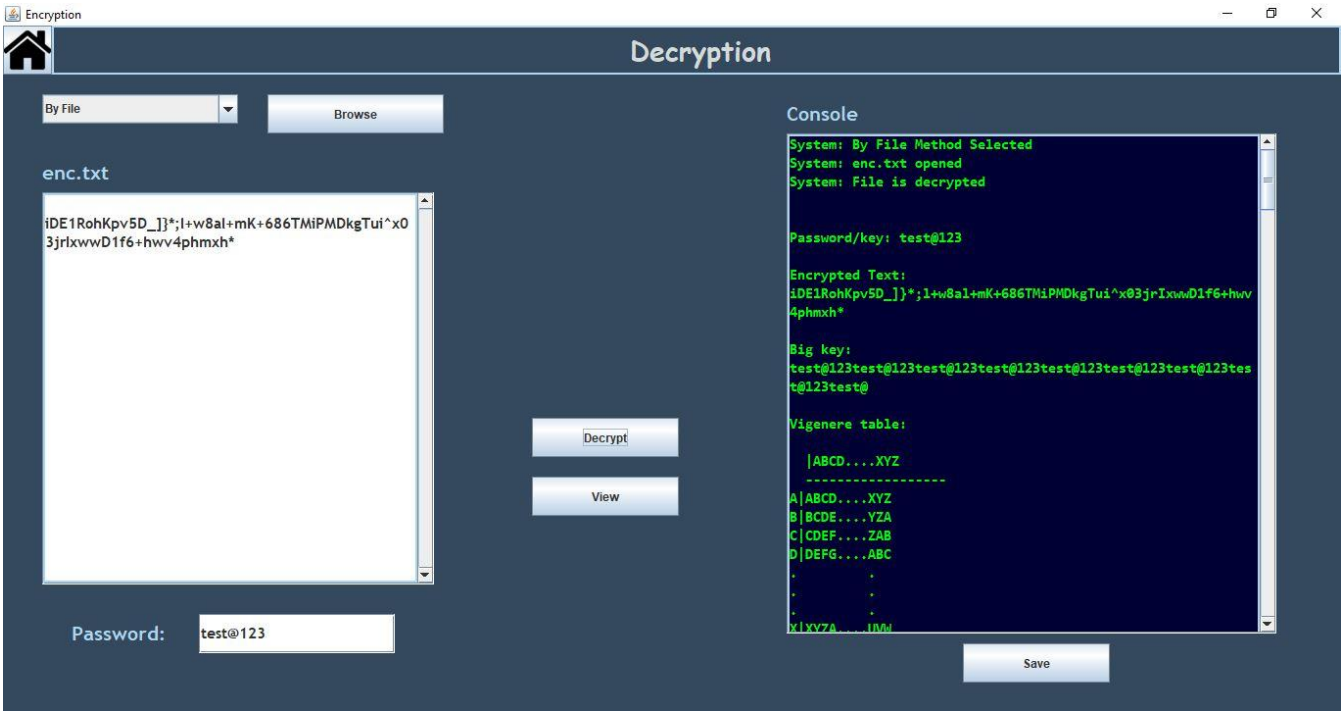




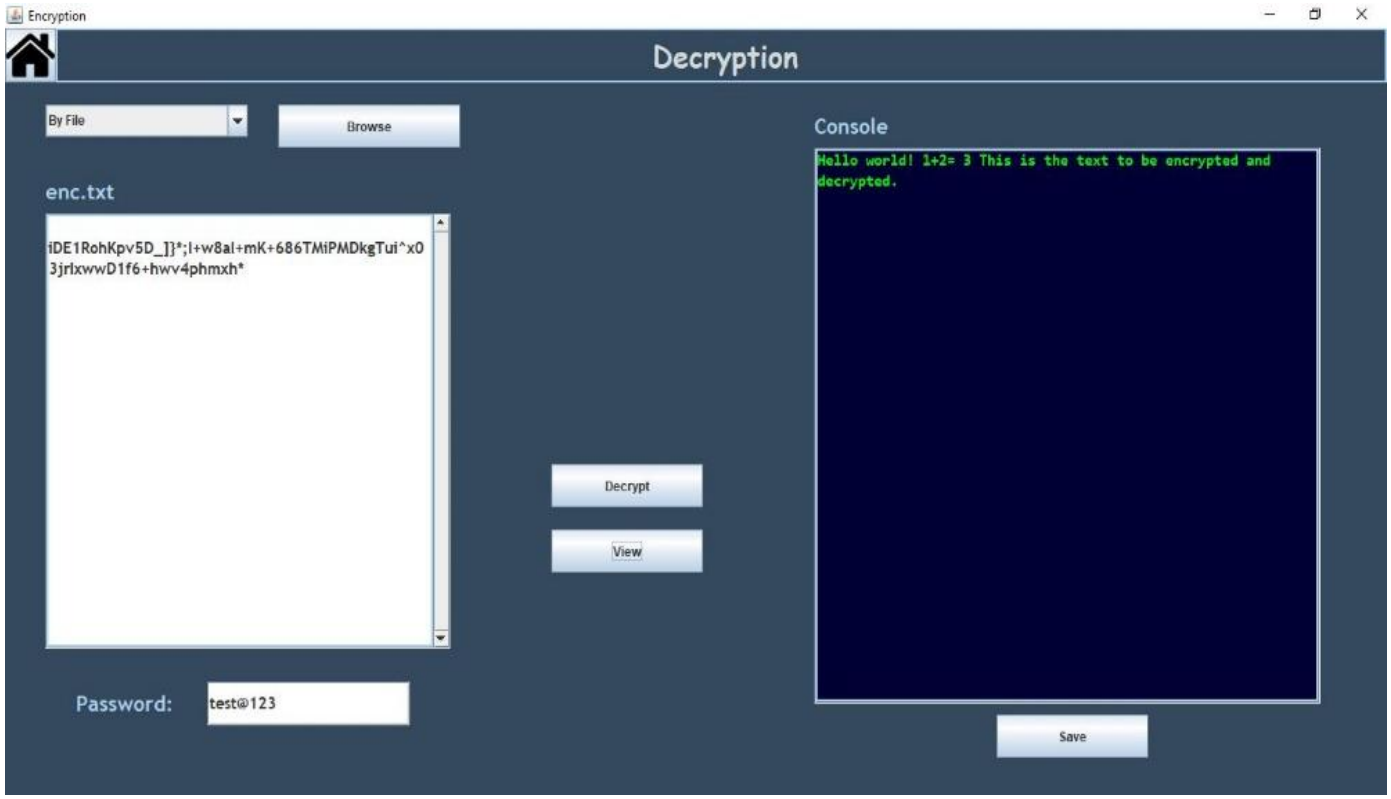


Decryption Screen:

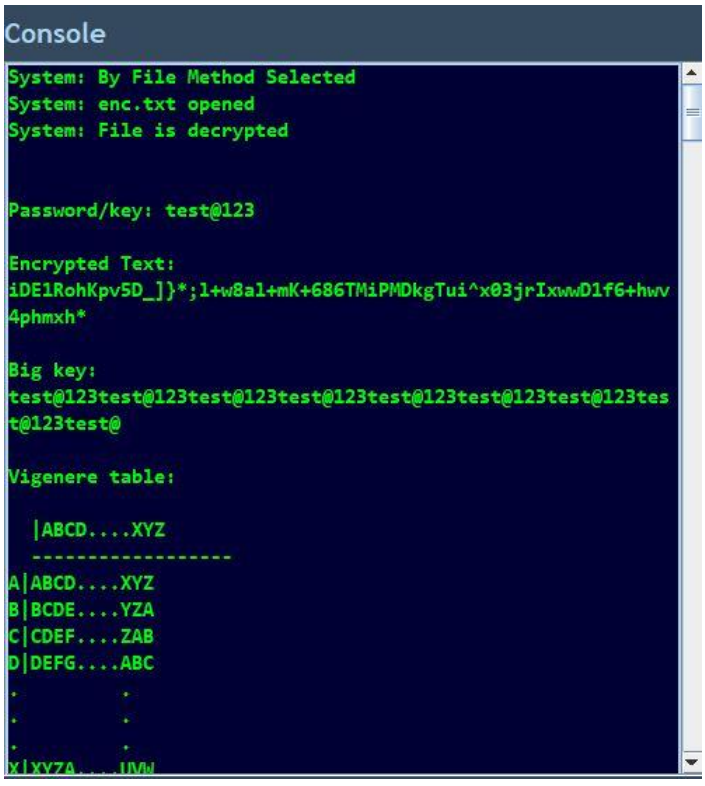
User can select one of the two method. On Selecting "By file" method, "Browse" button will appear, on pressing it user can select encrypted text file from device and have to enter the same password which was used for encrypting the same text, decrypt it by pressing "Decrypt" button.

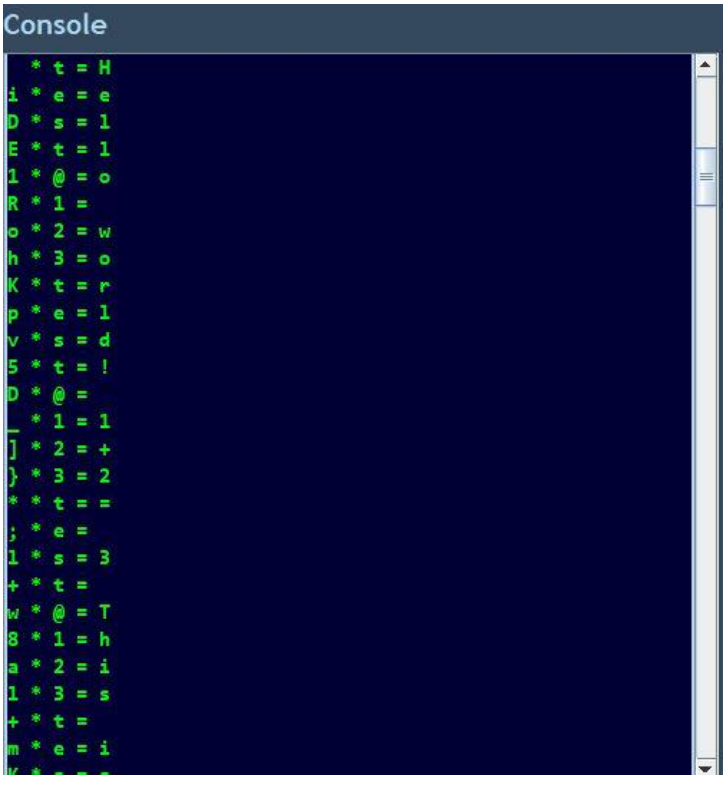


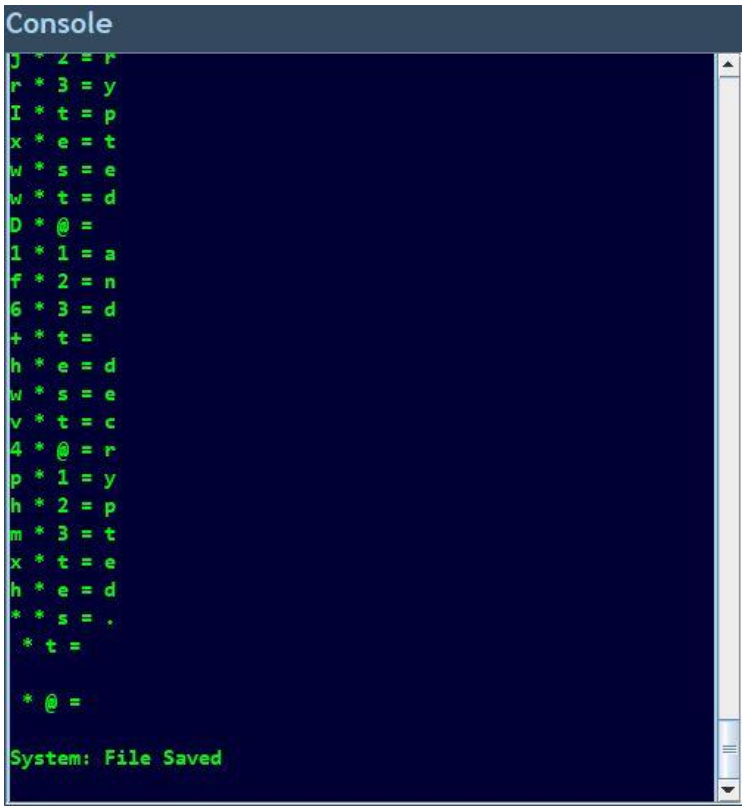
On clicking “View”, decrypted text can be seen and can be saved using “Save” button.



Steps of decryption:







Scope of improvements:

- Instead of just one algorithm, users can be provided a drop-down for selecting one of many available algorithms for encryption/decryption.
- Can be upgraded for encrypting/decrypting non-textual data like image, audio etc.